**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | | |
|---|---|---|
| **TIMOTHY ARNDT, individually and on behalf of all others similarly situated,** | * | |
| **Plaintiff** | * | |
| | * | **Civ. No. MJM-23-2842** |
| **v.** | * | |
| **GOVERNMENT EMPLOYEES INSURANCE COMPANY,** | * | |
| **Defendant.** | * | |

* * * * * * * *

## MEMORANDUM

Plaintiff Timothy Arndt ("Plaintiff") filed this putative class action against defendant Government Employees Insurance Company ("GEICO" or "Defendant") for allegedly tracking Plaintiff's and proposed class members' electronic activity on Defendant's website. *See* ECF No. 1 (Compl.). Specifically, Plaintiff asserts claims for violation of the Pennsylvania Wiretap and Electronic Surveillance Control Act ("PWESCA"), 18 Pa. C.S. § 5701, *et seq*. (Count I); Invasion of Privacy – Pennsylvania Intrusion Upon Seclusion (Count II); and violation of the Maryland Wiretapping and Electronic Surveillance Act ("MWESA"), Md. Code Ann., Cts. & Jud. Proc. § 10-401, *et seq.* (Count III).

This matter is before the Court on Defendant's Motion to Dismiss (ECF No. 15). The motion is fully briefed and ripe for disposition. No hearing is necessary. See Loc. R. 105.6 (D. Md. 2023). For the reasons stated below, the Court will GRANT the motion, and the Complaint will be dismissed without prejudice.

## I. BACKGROUND

Defendant is an insurance provider organized in Nebraska with its corporate headquarters in Maryland. Compl. ¶ 20. Defendant's website allows customers to shop for auto insurance by filling out online forms. *Id.* ¶¶ 25, 27. In or around January 2023, Plaintiff visited Defendant's website from Pennsylvania. *Id.* ¶¶ 26, 29. Plaintiff filled out an auto insurance quote form, which required him to input "personalized and sensitive information," including his social security number, contact information, vehicle and insurance information, marital status and spousal information, and gender identity. *Id.* ¶¶ 27–28, 46. Plaintiff was unaware, however, that the information he provided on Defendant's website—as well as the mouse clicks, keystrokes, and copy and paste actions—was collected by a third-party "Session Replay" software that intercepts users' electronic communications on Defendant's website. *Id.* ¶¶ 2–3, 30–31.

Defendant utilizes Session Replay software on its website through a third-party provider, Quantum Metric. *Id.* Quantum Metric collects data such as "mouse movements, keystrokes and clicks, search terms, content viewed, and personal information inputted by the website visitor . . . ." *Id.* ¶ 9. "The purported use of session replay technology is to monitor and discover broken website features." *Id.* ¶ 10. Plaintiff alleges, however, that the data collection "far exceeds the stated purpose and [users'] reasonable expectations . . . ." *Id.* Plaintiff alleges that his collected information was sent to Quantum Metric's servers. *Id.* ¶¶ 30–31.

Defendant factually disputes Plaintiff's allegations. Defendant submits the declaration of Christopher Jones, a Senior Director of Design at GEICO. Jones Decl. (ECF No. 15-2) ¶ 1. Jones avers that he is "the business owner for GEICO's service agreement with Quantum Metric." *Id.* Jones states that "all personally identifying information ('PII') was encrypted and pseudonymized before transmission to Quantum Metric." *Id.* ¶ 5. He states that, while Quantum Metric captures

user interactions including "clicks, scrolling, mouse movement, and masked keystrokes[,]" the "end user's session is identified using a random number, and any PII typed by an end user is encrypted on that end user's client device before reaching Quantum Metric." *Id.* ¶ 7. Further, "Quantum Metric also deploys a default 'do not capture' setting on GEICO's website, which automatically blocks the capture of any sensitive data (e.g. social security numbers, payment information, etc.)." *Id.* ¶ 11. Regarding other, non-sensitive PII, Quantum Metric pseudonymizes data "on the end user's client device before transmission to Quantum Metric's servers." *Id.* ¶ 12 (emphasis omitted).

Plaintiff filed suit in this Court on October 19, 2023. Defendant filed its Motion to Dismiss (ECF No. 15), to which Plaintiff responded (ECF No. 18), and Defendant replied (ECF No. 19). Defendant and Plaintiff each filed a notice of supplemental authority (ECF Nos. 21, 22), which this Court considered in rendering this decision.

## II. LEGAL STANDARD

### A. Rule 12(b)(6)

A motion to dismiss under Rule 12(b)(6) of the Federal Rules of Civil Procedure constitutes an assertion by a defendant that, even if the facts alleged by a plaintiff are true, the complaint fails as a matter of law "to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). For a complaint to survive a 12(b)(6) motion to dismiss, a plaintiff must plead enough factual allegations "to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

When considering a motion to dismiss, a court must take the factual allegations in the complaint as true and draw all reasonable inferences in favor of the plaintiff. *King v. Rubenstein*, 825 F.3d 206, 212 (4th Cir. 2016). But "a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action's elements will not do." *Twombly*, 550 U.S. at 555 (cleaned up). A complaint must contain factual allegations sufficient "to raise a right to relief above the speculative level." *Id.* "[T]ender[ing] 'naked assertion[s]' devoid of 'further factual enhancement'" does not suffice. *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557) (third alteration in *Iqbal*).

**B. Rule 12(b)(1)**

A defendant may move to dismiss a complaint for lack of subject matter jurisdiction under Rule 12(b)(1). *See Barnett v. United States*, 193 F. Supp. 3d 515, 518 (D. Md. 2016). "The plaintiff bears the burden of proving, by a preponderance of evidence, the existence of subject matter jurisdiction." *Mayor & City Council of Balt. v. Trump*, 416 F. Supp. 3d 452, 479 (D. Md. 2019). "A challenge to subject matter jurisdiction under Rule 12(b)(1) may proceed in one of two ways: either a facial challenge . . . or a factual challenge." *Id.* (citations omitted) (internal quotations omitted). A facial challenge asserts "that the allegations pleaded in the complaint are insufficient to establish subject matter jurisdiction." *Id.* A defendant's facial challenge "will be evaluated in accordance with the procedural protections afforded under Rule 12(b)(6), which is to say that the facts alleged in the Complaint will be taken as true . . . ." *In re Jones v. Md. Dept. of Pub. Safety*, No. 1:21-cv-01889-JRR, 2024 WL 493269 at *3 (D. Md. Feb. 8, 2024).

A factual challenge, on the other hand, asserts "that the jurisdictional allegations of the complaint are not true." *Trump*, 416 F. Supp. 3d at 479 (cleaned up) (quoting *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009)). In a factual challenge, the court "is entitled to decide disputed issues of fact with respect to subject matter jurisdiction. . . . In that circumstance, the

court may regard the pleadings as mere evidence on the issue and may consider evidence outside the pleadings without converting the proceeding to one for summary judgment." *Id.* (internal quotation marks and citations omitted); *see also U.S. ex rel. Vuyyuru v. Jadhav*, 555 F.3d 337, 348 (4th Cir. 2009) (court may consider evidence outside the pleadings, such as affidavits). However, "[i]f the jurisdictional facts are so intertwined with the facts upon which the ultimate issues on the merits must be resolved, . . . the entire factual dispute is appropriately resolved only by a proceeding on the merits . . . ." *Id.* (internal quotation marks omitted) (quoting *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982)).

## III. DISCUSSION

### A. Relevant Law

The three-count Complaint asserts causes of action under MWESA, PWESCA, and intrusion upon seclusion under Pennsylvania law. Under the MWESA:

> (a) Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this subtitle shall have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use the communications, and be entitled to recover from any person:
>
> (1) Actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;
>
> (2) Punitive damages; and
>
> (3) A reasonable attorney's fee and other litigation costs reasonably incurred.

Md. Code Ann., Cts. & Jud. Proc. § 10-410.[1]

PWESCA states that "[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. Cons. Stat. § 5725(a) (2024). To establish a PWESCA violation, a plaintiff must show:

> (1) that [the claimant] engaged in a communication; (2) that he possessed an expectation that the communication would not be intercepted; (3) that his expectation was justifiable under the circumstances; and (4) that the defendant attempted to, or successfully intercepted the communication, or encouraged another to do so.

*Kelly v. Carlisle*, 622 F.3d 248, 257 (3d Cir. 2010) (quoting *Agnew v. Dupler*, 553 Pa. 33, 717 A.2d 519, 522 (Pa. 1998)); *see also Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 130 (3rd Cir. 2022) (communication is "intercepted" from the location of the user's browser).

Finally, in Pennsylvania,[2] intrusion upon seclusion is the "obtaining or intercepting private, personal communications or information about a person in a matter that is highly offensive or unreasonable." *In re BPS Direct, LLC*, 705 F. Supp. 3d 333, 351 n.110 (E.D. Pa. 2023) (citation omitted).

---

[1] Maryland courts have found that MWESA does not have extraterritorial effect. *See Sprye v. Ace Morot Acceptance Corp.*, No. 423332-V, 2017 WL 11633219, at *3 (Md. Cir. Ct. 2017) (citation omitted); *Chairman of Bd. of Tr. of Emps.' Ret. Sys. v. Waldron*, 401 A.2d 172, 184 (Md. 1979) (holding that, unless the "intent to the contrary is expressly stated, acts of [the Maryland] legislature will be presumed not to have any extraterritorial effect") (quoting *Sandberg v. McDonald*, 248 U.S. 185, 195 (1918)).

[2] The Court must "apply the substantive law of the state of the 'place of harm.'" *Skapinetz v. CoesterVMS.com, Inc.,* Civ. No. PX-17-1098, 2018 WL 805393, at *6 (D. Md. Feb. 9, 2018). Plaintiff resides in Pennsylvania and was in Pennsylvania when he accessed Defendant's website, so Pennsylvania is the place of harm. *See* Compl. ¶¶ 19, 29.

**B. Standing**

In its Rule 12(b)(1) motion, Defendant argues Plaintiff lacks standing to sue because he has not established an injury in fact. *See* ECF No. 15. Defendant argues that Plaintiff cannot establish standing facially "based on non-sensitive, non-personal information" that Defendant collected. *Id.* at 20. In its factual challenge, Defendant maintains that Quantum Metric never received any sensitive personal information that Plaintiff entered into Defendant's website because any such information was encrypted. *Id.* at 16–17. Finally, Defendant argues that Plaintiff's allegedly heightened risk of identity theft fails to satisfy the *Clapper* test for an imminent injury-in-fact. *Id.*; *see also Clapper v. Amnesty Int'l, Inc.*, 568 U.S. 398, 414 n.5 (2013).

The United States Constitution extends judicial power to the courts to decide actual cases and controversies. *Spokeo v. Robins*, 578 U.S. 330, 337 (2016). The requirement of Article III standing ensures that the federal courts do not extend their power beyond actual cases and controversies. *Id.* at 338 (citations omitted). The Supreme Court has identified three elements of standing to ensure courts are adjudicating constitutionally compliant cases. *Id.* "The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Id.* (quoting *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560–61 (1992)). The plaintiff bears the burden of establishing those elements; at the pleading stage, he must clearly allege facts in support of each element. *Id.* (citing *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231 (1990)).

To establish injury in fact, "a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560). An injury is particularized when it "affect[s] the plaintiff in a personal and individual way." *Id.* (citations omitted). An injury is concrete when it actually exists and is "real, not abstract." *Straubmuller v.*

*Jetblue Airways Corp.*, Civ. No. DKC-23-384, 2023 WL 5671615, at *2 (D. Md. Sept. 1, 2023) (quoting *Spokeo*, 578 U.S. at 337) (cleaned up). Concrete injuries can be tangible, like money, or intangible, like reputational harm. *Id*. (citing *TransUnion LLC v. Ramirez*, 594 U.S. 413, 414 (2021)). "In a class action, [courts] analyze standing based on the allegations of personal injury made by the named plaintiffs." *Beck v. McDonald*, 848 F.3d 262, 269 (4th Cir. 2017).

In this case, Plaintiff alleges both intangible harm (i.e., invasion of privacy) and tangible harm (i.e., increased risk of "identity theft, online scams, and other unwanted behavior"). Compl. ¶¶ 11, 17. The Court will address each in turn.

**1. Intangible Harm**

Intangible harms may be "concrete" if they bear "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. . . . Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." *TransUnion* 594 U.S. at 425 (citations omitted). "A plaintiff proceeding under a statutory cause of action whose injury has 'a close historical or common-law analogue' for which courts have traditionally provided a remedy has standing even if the injury alone does not satisfy Article III standing requirements." *Straubmuller*, 2023 WL 5671615, at *2 (quoting *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921 (4th Cir. 2022)). Notably, the harm asserted need not be "an exact duplicate" of its historical or common-law analogue. *TransUnion*, 594 U.S. at 433.

Even though the legislature may elevate previously existing harms to actionable status, "it may not simply enact an injury into existence . . . ." *TransUnion*, 594 U.S. at 426. In other words, "an important difference exists between (i) a plaintiff's statutory cause of action to sue a defendant over the defendant's violation of federal law, and (ii) a plaintiff's suffering concrete harm because of the defendant's violation of federal law." *TransUnion*, 594 U.S. at 426–27; *see also Spokeo*, 578 U.S. at 341 (holding that a plaintiff cannot "allege a bare procedural violation, divorced from

any concrete harm, and satisfy the injury-in-fact requirement of Article III"). Thus, courts must still "independently decide whether a plaintiff has suffered a concrete harm under Article III . . . ." *Id.* at 426.

In *TransUnion*, the class plaintiffs alleged that a credit reporting agency mistakenly added an alert to consumer files indicating that the consumer was a "potential match" with individuals on a national security threat list. 594 U.S. at 420. For most consumers, the credit agency simply maintained the alert internally without dissemination. *Id.* at 421. For others, the agency distributed the reports to creditors. *Id.* The plaintiffs sued under the Fair Credit Reporting Act (FCRA), arguing that their injuries bore a "close relationship" to the traditional harm associated with defamation. *Id.* at 432. Defendant argued that, because defamation requires actual falsity, and the alerts only denoted "*potential* matches," the information at issue was not "technically false" and therefore did not bear a close relationship to defamation. *Id.* at 433. The Supreme Court disagreed, finding that the alleged harm bore "a sufficiently close relationship to the harm from a false and defamatory statement." *Id.*[3]

Thus, in this case, Plaintiff's alleged intangible injury is adequately concrete to confer standing if it bears a sufficiently close relationship to a common-law analogue. Plaintiff argues his injury is analogous to the harm from intrusion upon seclusion. ECF No. 18 at 17. Both Pennsylvania and Maryland follow the Restatement (Second) of Torts formulation of intrusion upon seclusion. *See Pro Golf Mfg., Inc. v. Trib. Rev. Newspaper Co.*, 809 A.2d 243, 247 (Pa. 2002); *Furman v. Sheppard*, 744 A.2d 583, 585 (Md. 2000). The Restatement (Second) § 652B provides:

[3] Critically, however, because publication is "essential to liability" for defamation, the Court held that "[t]he mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." *Id.* at 434.

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

The requirement that the intrusion be upon private affairs or concerns "confirms that the nature of the information is paramount." *Cook v. GameStop, Inc.*, 689 F. Supp. 3d 58, 65 (W.D. Pa. 2023). "A legitimate expectation of privacy is the touchstone of the tort of intrusion upon seclusion." *Whye v. Concentra Health Servs., Inc.*, Civ. No. ELH-12-3432, 2013 WL 5375167, at *14 (D. Md. Sept. 24, 2013), *aff'd*, 583 F. App'x 159 (4th Cir. 2014) (quoting *Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 877 (8th Cir. 2000). Thus, for Plaintiff's intangible injury to be sufficiently concrete, he must establish that he had a reasonable expectation of privacy in the communications allegedly intercepted by Defendant.[4]

In the instant case, Plaintiff alleges Defendant collected information like "mouse movements, keystrokes and clicks, search terms, [and] content viewed" by Plaintiff on Defendant's website. Compl. ¶ 9. Plaintiff further alleges he communicated the following information on Defendant's website:

> 1) his zip code; 2) name; 3) birthdate; 4) address; 5) the type of car he had; 6) whether he owned, financed, or leased his vehicle; 7) whether his vehicle was used primarily to commute, for pleasure, or for business; 8) details on his commuting; 9) his approximate annual mileage; 10) the length of time he owned his car; 11) his gender identity; 12) his marital status; 13) his social security number; 14) whether he owned or rented his home; 15) details about his current insurance; 16) whether he was licensed before age 29 in the US or Canada; 17) his highest level of education; 18) whether he had government or military affiliations; 19) his spouse's name and personal details; 20) his accident and traffic history; 21) group

[4] "To find that conduct is an unwarranted invasion of a plaintiff's privacy, both Maryland and Pennsylvania Courts engraft into the common law definition of 'privacy' the 'reasonable expectation of privacy' standard animating the Fourth Amendment to the Constitution of the United States. . . . That is, courts consider whether the privacy alleged to have been invaded is one protected from similar, governmental intrusion under the Fourth Amendment." *Demo v. Kirksey*, No. 8:18-CV-00716-PX, 2018 WL 5994995, at *3 (D. Md. Nov. 15, 2018) (citing cases).

> affiliations such as alumni associations; and 22) his email and phone number.

Compl. ¶ 28. None of the above information is sufficiently "intimate or personal" to justify a legitimate expectation of privacy.

First, Plaintiff cannot establish a concrete injury based on Defendant's alleged collection of mere website activity, such as mouse movements, keystrokes and clicks, search terms, or content viewed by Plaintiff on Defendant's website. Such information does not convey any personal, private, or identifying information. Rather, this information is comparable to that which would reflect "public shopping behavior in the physical world . . . ." *Cook*, 689 F. Supp. 3d. at 66 (comparing online shopping behavior to that which occurs at a brick-and-mortar store). Several other courts have dismissed cases involving Session Replay software for lack of standing where plaintiffs do not allege that any private information was intercepted. *See, e.g.*, *Hernandez v. Noom, Inc.*, Civ. No. JRR-23-641, 2023 WL 8934019, at *8 (D. Md. Dec. 27, 2023) ("Absent allegations regarding 'the specific kinds of captured personal information implicating a substantive privacy interest,' Plaintiff fails to adequately allege that she suffered an intangible injury . . . ."); *Straubmuller*, 2023 WL 5671615, at *4; *Lightoller v. Jetblue Airways Corp.*, No. 23-CV-00361-H-KSC, 2023 WL 3963823, at *5 (S.D. Cal. June 12, 2023) ("Plaintiff does not allege that Defendant recorded or collected any of her personal information."); *Adams v. PSP Grp., LLC*, 691 F. Supp. 3d 1031, 1041 (E.D. Mo. 2023) (observing that several district courts have held that, "where there are no allegations that the plaintiff shared personal or sensitive information on the website in question, the plaintiff has not adequately alleged a concrete harm to support Article III standing").

Plaintiff does allege, however, that Defendant collected certain personal identifying information. Some courts have found that the "unlawful disclosure of legally protected

information" is enough to confer standing. *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 274 (3d Cir. 2016). But the intrusion upon "communications that do not involve personal information, personally identifiable information, or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury." *Massie v. Gen. Motors LLC*, No. CV 21-787-RGA, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022). Further, "the collection of basic contact information by Session [Replay] software . . . [is] not a concrete harm[]." *Smidga*, 2024 WL 1485853, at *4 (citing cases); *see also Phillips v. U.S. Customs & Border Prot.*, 74 F.4th 986, 996 (9th Cir. 2023) (holding that plaintiffs did not have standing because they failed to demonstrate that the information at issue "is so sensitive that another's access to that information 'would be highly offensive to a reasonable person, . . . or otherwise gives rise to reputational harm or injury to privacy interests"). Rather, to be injurious, the intercepted communications must be "generally considered private." *Id.* (citation omitted).

In this case, most of the information Plaintiff alleges Defendant collected—such as basic contact information, marital status and spousal information, vehicle and driving history, highest level of education, and governmental, military, and group associations—is exactly that which is commonly provided to private parties, particularly for purposes of acquiring insurance. This information is not highly sensitive and, to a reasonable person, would not generally be considered private.

In his response to the motion, Plaintiff asserts a privacy interest in his gender identity as a male and marital status.[5] ECF No. 18 at 19–20.[6] Even if Plaintiff had a legitimate expectation of privacy in this information, his claims would not survive Defendant's factual challenge that the at-issue information was encrypted and, therefore, not disseminated to any third parties. *See Smidga*, 2024 WL 1485853, at *5 (dismissing case where the plaintiff failed to adequately respond to the defendant's "sworn assertions that no personalized data was recorded"). Defendant's agent, Christopher Jones, states in his declaration that "all personally identifying information ('PII') was encrypted and pseudonymized before transmission to Quantum Metric." *Id.* ¶ 5. He states that "the end user's session is identified using a random number, and *any PII typed by an end user is encrypted* on that end user's client device before reaching Quantum Metric." *Id.* ¶ 7 (emphasis added). Even information that is deemed "not sensitive" is encrypted before it is transferred to Quantum Metric's server. *Id.* ¶ 10.

In light of the foregoing, Plaintiff has failed to demonstrate that he had a legitimate expectation of privacy in the information he communicated on Defendant's website. Insofar as he had a privacy interest in such information, Jones's declaration confirms that the information

---

[5] Plaintiff does not make any argument specifically regarding the disclosure of his social security number. *See generally* ECF No. 18. The Fourth Circuit recently held that a plaintiff who intentionally handed over their social security number on one website did not plead anything close to intrusion upon seclusion when that information was allegedly shared with a website. *O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 241, 245–46 (4th Cir. 2023).

[6] Cases cited by Plaintiff do not support his argument. In *Roe by & through Roe v. Critchfield*, the court specifically noted the dearth of case law recognizing "a true 'privacy' interest in one's gender identity" and found the plaintiffs unlikely to succeed on the merits of their due process claim challenging disclosure of such information. Civ. No. 1:23-00315-DCN, 2023 WL 6690596, at *16 (D. Idaho Oct. 12, 2023). In *Grimes v. County of Cook*, the defendant conceded that its public disclosure of the plaintiff's transgender status at work would be highly offensive to a reasonable person. 455 F. Supp. 3d. 630 at 640 (N.D. Ill. 2020).

Plaintiff communicated was protected from disclosure. Accordingly, Plaintiff has failed to demonstrate that he suffered an intangible harm sufficient to confer standing.

**2. Tangible Harm**

Plaintiff also alleges that Defendant's utilization of Session Replay software exposes him to increased risk of tangible harms, such as "identity theft, online scams, and other unwanted behavior." Compl. ¶ 11. Because "Defendant's conduct is ongoing," Plaintiff seeks "declaratory and injunctive relief to prevent future interception of their communications." *Id.* ¶ 117. Defendant argues the alleged risk of future harm is neither "substantial" nor "clearly impending" and, therefore, fails to confer standing. ECF No. 15 at 21–22.

Threatened rather than actual injury can satisfy Article III standing. *See Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 477, (1982); *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 160 (4th Cir. 2000). But, as the Supreme Court has emphasized repeatedly, "threatened injury must be *certainly impending* to constitute injury in fact," and "[a]llegations of *possible* future injury are not sufficient." *Clapper*, 568 U.S. at 409 (internal quotation marks and citation omitted) (alteration and emphasis in original). A threatened injury cannot be premised on a "highly attenuated chain of possibilities." *Id.*

In cases involving the future risk of identity theft, the Fourth Circuit has held that a plaintiff's claims are "too speculative" unless the plaintiff alleges that his information was "intentionally targeted" or misused. *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017). *Compare Hutton v. Nat'l Bd. of Examiner in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (holding that plaintiffs alleged an injury-in-fact where they "allege that they have already suffered actual harm in the form of identity theft and credit card fraud"); *with O'Leary*, 60 F.4th at 244–45 (holding that plaintiff failed to allege a sufficient threatened injury where he could not "connect

the alleged statutory violation to an increased risk of identity theft without a Rube Goldberg-type chain reaction").

In this case, Plaintiff has not alleged that his information was intentionally targeted or misused. In fact, the Complaint specifically recognizes the speculative nature of Plaintiff's claims. It states that "the collection and storage of page content *may* cause sensitive information . . . to leak to additional third parties. This *may* expose website visitors to identity theft, online scams, and other unwanted behavior." Compl. ¶ 11 (emphasis added). This is exactly the type of chain reaction that the Supreme Court deemed too speculative in *Clapper*.

Because Plaintiff fails to establish an injury-in-fact necessary to confer Article III standing,[7] his claims will be dismissed. It is therefore unnecessary for the Court to address Defendant's motion to dismiss for failure to state a claim.

## IV. CONCLUSION

For the reasons stated herein, Defendant's Motion to Dismiss (ECF No. 15) will be GRANTED under Rule 12(b)(1), and the Complaint will be dismissed without prejudice.

A separate Order will issue.

9/26/24
Date

Matthew J. Maddox
United States District Judge

[7] For this reason, Plaintiff is not entitled to injunctive or declaratory relief. *See, e.g.*, *Beck*, 848 F.3d 262, 277 (4th Cir. 2017) ("A plaintiff who seeks . . . to enjoin a future action must demonstrate that he 'is immediately in danger of sustaining some direct injury' as the result of the challenged official conduct.") (quoting *Lebron v. Rumsfeld*, 670 F.3d 540, 560 (4th Cir. 2012)); *Nat'l Fed'n of the Blind v. United States Dep't of Educ.*, 407 F. Supp. 3d 524, 535 (D. Md. 2019) (finding that plaintiff lacked standing to seek injunction or declaratory relief because the risk of future harm was "too speculative").